REMARKS

In the present application, claims 1-23 are pending. Claims 1-23 are rejected. As a result of this response, claims 1-23 are believed to be in condition for allowance.

Claim Objections

The Examiner objected to claims 8, 9, and 15 asserting that they are "substantial duplicates" of one another. Applicants respectfully disagree with the Examiner's assertion. Specifically, Applicants maintain that claims 8, 9, and 15 are each of a scope that is both well defined and different from that of the others.

Specifically, claim 8 is drawn to "an access network", claim 9 is drawn to "an access network element", and claim 15 is drawn to "a ciphering controller". As is evident, claim 8 does not specify in which network element the recited claim elements reside. In contrast, claim 9 makes explicit that the recited claim elements reside upon "an access network element". Lastly, claim 15 makes explicit that it is a "ciphering controller" that comprises the recited claim elements. As is therefore evident, each of claims 8, 9, and 15 are distinctly drawn to well defined, separate subject matter and, as such, are not "substantial duplicates" of each other. Applicants therefore respectfully traverse the Examiner's objection.

Claim Rejections – 35 USC § 102

The Examiner rejected claims 1-23 as being anticipated by Berenzweig (U.S. Patent 6,584,310). Specifically, the Examiner asserted that Berenzweig "discloses "a communication network [,] an access network element, or ciphering controller, and a method comprising a user equipment, an access network and a plurality of core networks, wherein said user equipment is configured to be simultaneously in communication with at least two of said plurality of core networks, said communication network comprising: Berenzweig discloses at least two networks wherein each has means of communicating separate ciphering communications to the access network that meets the recitation of means for communicating separate ciphering parameters to said access network from said at least two of said core networks, for example (see column 3, line 45 through column 4, line 7)". The Examiner further asserted that "Berenzweig discloses means

for receiving separate ciphering parameters to said access network from said at least two of said core networks, for example (see column 5, lines 20-23 and lines 5, 29-31)." Lastly, the Examiner asserted that "Berenzweig also discloses means for selecting either the triplets or shared secret key for ciphering between the user and the at least two of the core networks that meets the recitation of said access network comprising means for selecting one of said separate ciphering parameters for ciphering the communications between said user equipment and said at least two of said plurality of core networks in said access network, for example (see columns 3, line 45 through column 4, line 7 and see one example illustrated in column 6, lines 35-63)."

Applicants respectfully disagree with Examiner's characterization of the teachings of Berenzweig vis-à-vis the recitations of the claims. Claim 1 is taken as representative of distinctions over Berenzweig and recites:

> 1. A communication network comprising a user equipment, an access network and a plurality of core networks, wherein said user equipment is configured to be **simultaneously in communication with at least two of said plurality of core networks**, said communication network comprising:
> means for **communicating separate ciphering parameters** to said access network from said at least two of said core networks; and
> means for **selecting one of said separate ciphering parameters** for ciphering communications between said user equipment and said at least two of said plurality of core networks in said access network. (emphasis added).

As will be shown, Berenzweig does not teach or disclose user equipment "configured to be simultaneously in communication with at least two of said plurality of core networks", "communicating separate ciphering parameters to said access network", or "selecting one of said separate ciphering parameters".

Berenzweig discloses, in general, translation between different authentication schemes when a mobile station is roaming between networks. A first authentication scheme (triplets) is used in a first network and a second authentication scheme (shared secret data, SSD) is used in a second network. There is an authentication interoperability function (AIF) which translates between the first and second authentication schemes. (see abstract) In this manner, a mobile

station native to the second network may roam in the first network and authenticate itself towards the first network using the first authentication scheme.

For example, with reference to Fig. 9, Berenzweig shows a mobile station native to the second network 220 using SSD for authentication. The mobile station authenticates itself to the first network 218 using triplets for authentication. The Visitor Location Register requests a triplet from the AIF, which generates triplets from the SSD information received from the Home Location Register of the second network.

In contrast, claim 1 recites an access network over which the user equipment is "simultaneously in communication with at least two of said plurality of core networks". Berenzweig teaches the presence of two networks between which a mobile station roams. Berenzweig does not disclose a mobile station simultaneously in communication with at least two core networks when roaming in either of the two access networks. As a result, Berenzweig fails to teach or otherwise disclose user equipment "configured to be simultaneously in communication with at least two of said plurality of core networks" as claimed.

More fundamentally, Applicants respectively disagree with the Examiner's assertion that "Berenzweig discloses means for receiving separate ciphering parameters to said access network from said at least two of said core networks, for example (see column 5, lines 20-23 and lines 5, 29-31)." The Examiner's citation refers to Fig. 9. As is clear from the reference, as well as examination of Fig. 9, the VLR receives only one triplet from the AIF (see column 5, lines 20-21). Put simply, Berenzweig teaches that the AIF enables the same mobile station to be authenticated in disparate networks. The AIF is between the networks themselves (col. 3, lines 55-62, Figs. 7-11) and operates so that only one triplet is sent to the mobile sterminal. As such, Berenzweig discloses receiving only one ciphering parameter in the access network. Therefore, Berenzweig fails to teach "communicating separate ciphering parameters to said access network" as is claimed. Furthermore, as Berenzweig teaches the reception of only one ciphering parameter, there is no teaching of "selecting one of said separate ciphering parameters" as recited in claim 1.

Lastly, the Examiner references column 6, lines 35-63, which references Fig. 10, to support the assertion that "Berenzweig also discloses means for selecting either the triplets or shared secret key for ciphering between the user and the at least two of the core networks that

meets the recitation of said access network comprising means for selecting one of said separate ciphering parameters for ciphering the communications between said user equipment and said at least two of said plurality of core networks in said access network". In fact, Berenzweig discloses that the AIF receives two triplets from the HLR of the first network. However, both triplets are used to calculate the shared secret data SSD to be transmitted to the VLR of the second network. Therefore, the input ciphering parameter of the VLR is from only one network and, thus, teaches directly away from separate ciphering parameters from at least two core networks. Berenzweig thereby fails to once again teach "communicating separate ciphering parameters to said access network from said at least two of said core networks", and "selecting one of said separate ciphering parameters" as claimed.

For the aforementioned reasons, Berenzweig fails to teach or suggest numerous elements recited in claim 1. As a result, Applicants respectfully traverse the Examiner's grounds for rejection. Claim 1 is therefore in condition for allowance. As claims 8, 9, and 15 recite similar limitations, they are likewise deemd to be in condition for allowance for the reasons recited above with reference to claim 1. As all of claims 2-7, 10-14, and 16-23 depend upon claim 1, 8, 9, and 15, they are likewise in condition for allowance.

Respectfully submitted:

Jeffrey R. Ambroziak — Date: 6 Jul 05

Reg. No.: 47,387

Customer No.: 29683
HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203)925-9400
Facsimile: (203)944-0245
email: hsmith@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

7/7/2005 — Date

Claire F. Mann — Name of Person Making Deposit